PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-251375
(43)Date of publication of application : 06.09.2002

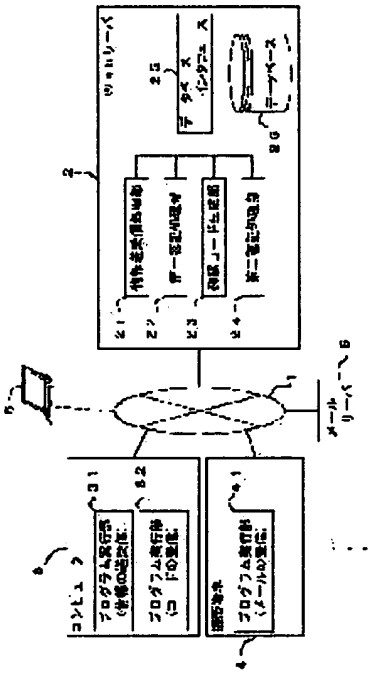
(51)Int.Cl. G06F 15/00
H04L 9/32

(21)Application number : 2001-044841
(22)Date of filing : 21.02.2001

(71)Applicant : NTT DATA CORP
(72)Inventor : GOHIYAKUDEN TAKAYUKI

(54) USER AUTHENTICATION SERVER IN COMMUNICATION NETWORK, INDIVIDUAL AUTHENTICATION METHOD AND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To eliminate illegal 'pretence' and to securely decide a user oneself.
SOLUTION: A Web server 2 receives ID and a password from the computer 3 of the user, collates them with ID and the password, which are stored in a database 26, and performs first authentication. When the first authentication succeeds, the Web server 2 transmits a confirmation code to an electronic mail address which is stored in the database 26 and which the user designates. The destination is a mail server 5. The user receives the confirmation code from the mail server 5 by using a portable terminal 4 and inputs it to a computer 3. The inputted confirmation code is returned to the Web server 2 as a return code. The Web server 2 collates the received confirmation code with the transmitted confirmation code. When they are matched, it is decided that second authentication is succeeded.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－251375
(P2002－251375A)
(43)公開日　平成14年９月６日(2002.9.6)

(51)Int.Cl.'	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０８５
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	５Ｊ１０４

審査請求　未請求　請求項の数５　ＯＬ　（全　９　頁）

(21)出願番号　特願2001－44841(P2001－44841)

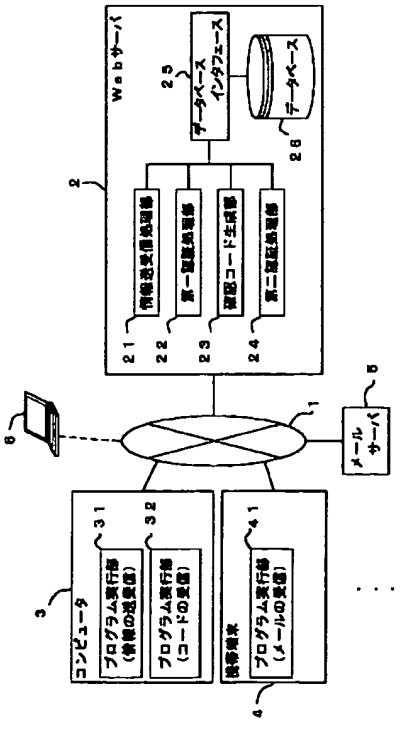
(22)出願日　平成13年２月21日(2001.2.21)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　五百田　孝行
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100095407
弁理士　木村　満

Ｆターム(参考)　5B085 AE01 AE23 BG07 CA04
5J104 AA07 AA12 KA01 KA06 MA02
NA05 PA07

(54)【発明の名称】　通信ネットワークにおけるユーザ認証サーバ、本人認証方法及びプログラム

(57)【要約】
【課題】　不正な「なりすまし」を排除して、ユーザ本人の確定を確実に行うことができるようにする。
【解決手段】　Ｗｅｂサーバ２は、ユーザのコンピュータ３からＩＤ及びパスワードを受け取り、データベース２６に記憶されているＩＤ及びパスワードと照合し、第一認証を行う。第一認証が成功したとき、Ｗｅｂサーバ２は確認コードを、データベース２６に記憶されているユーザ指定の電子メールアドレス宛てに送信する。宛先は、メールサーバ５である。ユーザは、携帯端末４を用いてメールサーバ５から確認コードを受信し、コンピュータ３に入力する。入力された確認コードは、返信コードとしてＷｅｂサーバ２に返信される。Ｗｅｂサーバ２は、受信した確認コードを、送信した確認コードと照合し、一致したときは、第二認証が成功したと判定する。



1

【特許請求の範囲】

【請求項１】通信ネットワークに接続され、当該通信ネットワークに接続されたユーザ端末との間で、当該ユーザ端末を使用するユーザの認証を行うためのユーザ認証サーバにおいて、

ユーザの認証コードと確認コード送信先とを対応付けて予め記憶する記憶手段と、

前記ユーザ端末から送信される認証コードを受信し、受信した認証コードを、前記記憶手段に記憶されている認証コードと照合することにより第１の認証を行う第１の認証手段と、

該第１の認証手段による認証が成功したとき、対応する確認コード送信先に、所定の確認コードを通知する確認コード通知手段と、

該確認コード通知手段による確認コード通知の応答としての返信コードを受信し、受信した返信コードを、通知した確認コードと照合することにより第２の認証を行う第２の認証手段と、

を備えたことを特徴とする通信ネットワークにおけるユーザ認証サーバ。

【請求項２】前記返信コードの送信元は、前記確認コード送信先と異なることを特徴とする請求項１に記載の通信ネットワークにおけるユーザ認証サーバ。

【請求項３】前記第２の認証手段は、受信した返信コードを、前記確認コード通知手段が通知した確認コードと照合した結果、返信コードと確認コードとの間に一定の相関がとれたときに第２の認証を行うものであることを特徴とする請求項１又は２に記載の通信ネットワークにおけるユーザ認証サーバ。

【請求項４】通信ネットワークにおける本人認証方法であって、

ユーザの認証データと確認コード送信先とを対応付けてユーザ認証サーバに予め記憶しておくステップと、

通信ネットワークを介して受信した認証データを、ユーザ認証サーバに記憶された認証データと照合することにより、認証コードの送り主がユーザ本人であるか否かの認証を行うステップと、

認証データの送信主がユーザ本人であるとの認証がなされたとき、通信ネットワークを介して、対応する確認コード送信先に所定の確認コードを通知するステップと、

該確認コード通知の応答としての返信コードを受信し、受信した返信コードを、通知した確認コードと照合することにより、前記認証コードの送り主が、前記確認コード送信先に所在するユーザ本人であるかどうかの認証を行うステップと、を備えたことを特徴とする通信ネットワークにおける本人認証方法。

【請求項５】通信ネットワークに接続されたコンピュータに、

ユーザの認証コードと確認コード送信先とを対応付けて予め記憶する手順、

2

通信ネットワークを介して認証コードを受信して、受信した認証コードを、記憶している認証コードと照合することにより、認証コードの送り主がユーザ本人であるか否かの認証を行う手順、

認証コードの送り主がユーザ本人であるとの認証がなされたとき、対応する確認コード送信先に、所定の確認コードを通知する手順、

確認コード通知の応答としての返信コードを受信して、受信した返信コードを、通知した確認コードと照合することにより、前記認証コードの送り主が、確認コード送信先に所在するユーザ本人であるか否かの認証を行う手順、を実行させるためのプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、通信ネットワークにおけるユーザ認証サーバ、本人認証方法及びプログラム（program）に関し、特に不正なりすましを防止する通信ネットワークにおけるユーザ認証サーバ、本人認証方法及びプログラムに関する。

【０００２】

【従来の技術】インターネットは、不特定多数の者が利用することのできる便利な通信ネットワークである。その反面、このインターネットでは、情報伝送路がネットワーク状になっているため、情報は数多くの中継点を経由する。このため、情報が第三者によって不正に盗み取られるという可能性も否定できない。

【０００３】このようなインターネットにおいて、不正を防止するためには、まず、通信相手がユーザ本人であるかどうかを確認する必要がある。従来、インターネット上の取引においては、本人認証として、ユーザのＩＤとパスワードを入力することによりユーザ本人であるかどうかの本人確認を行うのが一般的である。

【０００４】

【発明が解決しようとする課題】ところで、インターネット上では、ユーザのＩＤやパスワードを盗み、盗んだＩＤやパスワードを用いてユーザ本人になりすますような不正行為が見受けられる。このような行為はいわゆる「なりすまし」と呼ばれるものであり、従来の本人認証のやり方では、このような「なりすまし」を防止することは困難である。インターネットでは、この「なりすまし」が大きな脅威であり、このような不正を防止する必要がある。

【０００５】本発明は、このような従来の問題に鑑みてなされたもので、不正なりすましを防止することが可能な通信ネットワークにおけるユーザ認証サーバ、本人認証方法及びセキュリティプログラムを提供することを目的とする。

【０００６】

【課題を解決するための手段】上記目的を達成するため、本発明の第１の観点に係る通信ネットワークにおけ

るユーザ認証サーバは、通信ネットワークに接続され、当該通信ネットワークに接続されたユーザ端末との間で、当該ユーザ端末を使用するユーザの認証を行うためのユーザ認証サーバにおいて、ユーザの認証コードと確認コード送信先とを対応付けて予め記憶する記憶手段と、前記ユーザ端末から送信される認証コードを受信し、受信した認証コードを、前記記憶手段に記憶されている認証コードと照合することにより第１の認証を行う第１の認証手段と、該第１の認証手段による認証が成功したとき、対応する確認コード送信先に、所定の確認コードを通知する確認コード通知手段と、該確認コード通知手段による確認コード通知の応答としての返信コードを受信し、受信した返信コードを、通知した確認コードと照合することにより第２の認証を行う第２の認証手段と、を備えたものである。

【０００７】このような構成によれば、第１の認証手段による第１の認証が成功したときは、確認コードが送信される。確認コードは、対応するユーザの認証コードに対応した確認コード送信先に送信されるので、第三者がユーザの認証コードを盗んでユーザになりすますことにより、第１の認証がうまく成功したとしても、この第三者には、確認コードは届かない。確認コードが届かなければ、第三者は返信コードを送信することもできず、返信コードが受信されなければ、確認コードと返信コードとの照合を行うことはできず、第２の認証手段による第２の認証を行うことはできない。これにより、なりすましは排除され、不正が防止される。

【０００８】前記返信コードの送信元は、前記確認コード送信先と異なるようにしてもよい。また、前記第２の認証手段は、受信した返信コードを、前記確認コード通知手段が通知した確認コードと照合した結果、返信コードと確認コードとの間に一定の相関がとれたときに第２の認証を行うものであってもよい。

【０００９】本発明の第２の観点に係る通信ネットワークにおける本人認証方法は、ユーザの認証データと確認コード送信先とを対応付けてユーザ認証サーバに予め記憶しておくステップと、通信ネットワークを介して受信した認証データを、ユーザ認証サーバに記憶された認証データと照合することにより、認証コードの送り主がユーザ本人であるか否かの認証を行うステップと、認証データの送信主がユーザ本人であるとの認証がなされたとき、通信ネットワークを介して、対応する確認コード送信先に所定の確認コードを通知するステップと、該確認コード通知の応答としての返信コードを受信し、受信した返信コードを、通知した確認コードと照合することにより、前記認証コードの送り主が、前記確認コード送信先に所在するユーザ本人であるかどうかの認証を行うステップと、を備えたものである。

【００１０】本発明の第３の観点に係るプログラムは、通信ネットワークに接続されたコンピュータに、ユーザ

の認証コードと確認コード送信先とを対応付けて予め記憶する手順、通信ネットワークを介して認証コードを受信して、受信した認証コードを、記憶している認証コードと照合することにより、認証コードの送り主がユーザ本人であるか否かの認証を行う手順、認証コードの送り主がユーザ本人であるとの認証がなされたとき、対応する確認コード送信先に、所定の確認コードを通知する手順、確認コード通知の応答としての返信コードを受信して、受信した返信コードを、通知した確認コードと照合することにより、前記認証コードの送り主が、確認コード送信先に所在するユーザ本人であるか否かの認証を行う手順、を実行させるためのものである。

【００１１】

【発明の実施の形態】以下、本発明の実施の形態に係る通信ネットワークにおけるセキュリティシステムを図面を参照して説明する。図１は、本実施の形態に係るセキュリティシステムの構成を示すブロック図である。この実施の形態に係るセキュリティシステムは、インターネット１と、Ｗｅｂサーバ２と、コンピュータ３と、携帯端末４と、メールサーバ５と、を備えている。尚、コンピュータ６は、ユーザ本人になりすまして不正に情報を送受信しようとする第三者のコンピュータである。

【００１２】インターネット１は、情報を送受信するためのネットワークである。Ｗｅｂサーバ２は、インターネット１に接続されて、ユーザのＩＤ及びパスワード等の情報をＨＴＴＰ（HyperText Transfer Protocol）プロトコルに従って送受信するためのコンピュータである。

【００１３】Ｗｅｂサーバ２は、情報送受信処理部２１と、第一認証処理部２２と、確認コード生成部２３と、第二認証処理部２４と、データベースインタフェース２５と、データベース２６と、を備えて構成されている。

【００１４】情報送受信処理部２１は、ユーザのコンピュータ３との間で情報の送受信を行うものである。第一認証処理部２２は、ユーザから送信されたＩＤ、パスワードを、データベース２６に記憶されているユーザのＩＤ、パスワードと照合し、照合結果に基づいて第一認証を行うものである。

【００１５】確認コード生成部２３は、第一認証処理部２２によって第一認証が行われた後に、確認コードを自動的に生成するものであり、生成した確認コードをデータベースインタフェース２５を介してデータベース２６に記録する。確認コードは、後述するように、送り先のユーザと対応する記憶場所に記憶される。第二認証処理部２４は、ユーザに送信した確認コード及びユーザから返送された返信コードを照合し、照合結果に基づいて第二認証を行う処理部である。データベースインタフェース２５は、ユーザのＩＤ、パスワード、送信した確認コード等をデータベース２６に記録し、データベース２６から読み出すものである。

5

【００１６】データベース２６は、ユーザのＩＤ、パスワード、ユーザが指定した電子メールアドレス等のユーザ情報をユーザごとに対応付けて記憶しておくためのものである。図２は、データベース２６に記憶されたユーザ情報の一例を示す説明図である。図２に示すように、データベース２６には、ユーザ毎にユーザエリアが設けられ、各ユーザエリアには、ユーザ名、ユーザのＩＤ、パスワード、電子メールアドレス等が記憶される。前述の確認コード等もこのユーザエリアに記憶される。

【００１７】電子メールアドレスは、認証成功のメッセージ、確認コード等、ユーザに送るメールの送り先を指定するためのものであり、ユーザ自身によって指定される。この電子メールアドレスによってメールサーバ５が指定される。

【００１８】コンピュータ３は、ユーザが使用するコンピュータであり、インターネット１に接続されている。コンピュータ３は、プログラム実行部３１及びプログラム実行部３２を有している。プログラム実行部３１は、情報の送受信処理プログラムを実行する実行部である。この送受信処理プログラムは、Ｗｅｂサーバ２との間で送受信を行えるようにブラウザ機能を有している。また、プログラム実行部３２は、メールサーバ５に届けられたメールを受信するための受信処理プログラムを実行する実行部である。

【００１９】図３は、コンピュータ３のハードウェア構成を示すブロック図である。コンピュータ３は、ＣＰＵ（Central Processing Unit）３３と、ＲＯＭ（Read Only Memory）３４と、ＲＡＭ（Random Access Memory）３５と、ディスプレイ３６と、キーボード３７と、マウス３８と、ＨＤＤ（Hard Disk Drive）３９と、を備えている。

【００２０】ＣＰＵ３３は、プログラム実行部３１及びプログラム実行部３２を実行するためのものである。ＲＯＭ３４は、プログラム実行部３１及びプログラム実行部３２によって実行されるプログラムを格納しておくためのメモリである。ＲＡＭ３５は、プログラム実行部３１及びプログラム実行部３２の実行に必要なデータを一時格納しておくためのためのメモリである。

【００２１】ディスプレイ３６は、Ｗｅｂサーバ２から送信された情報を表示し、データ入力の案内を表示するためのものである。キーボード３７は、ＩＤ、パスワードを入力するためのものである。マウス３８は、ディスプレイ３６に表示された各ボタンをクリックするためのものである。ＨＤＤ３９は、Ｗｅｂサーバ２との間で送受信した情報を格納しておく記憶装置である。

【００２２】携帯端末４は、携帯可能な端末であり、しかも通信機能を備えたものである。携帯端末４には、例えば、携帯電話、ＰＨＳ（Personal Handyphone System）、ＰＤＡ（Personal Digital Assistance）、モバイル（Mobile）コンピュータが含まれる。この携帯端末４

6

は、プログラム実行部４１を有している。プログラム実行部４１は、メールサーバ５に届けられたメールを受信するための受信処理プログラムを実行する実行部である。

【００２３】携帯端末４には、液晶ディスプレイと、ダイヤルキーと、スピーカと、マイクと、アンテナと、が備えられている。液晶ディスプレイは、送受信情報、操作情報等を表示するためのものである。ダイヤルキーは、発呼手続等を行うためのものである。スピーカは、受信した音声を出力するためのものである。マイクは、ユーザの声を入力するためのものである。アンテナは、通話信号を送受信するためのものである。メールサーバ５は、Ｗｅｂサーバ２から送信されたメール、確認コードを記憶しておくものである。

【００２４】次に、本実施の形態に係るなりすましを排除するための本人認証方法について説明する。図４は、本実施の形態に係るＷｅｂサーバ２、コンピュータ３及び携帯端末４の動作を示すフローチャートである。

【００２５】まず、コンピュータ３では、プログラム実行部３１が、Ｗｅｂサーバ２にログインの要求をする（ステップＳ１１）。Ｗｅｂサーバ２では、情報送受信処理部２１が、コンピュータ３から送信されたログイン要求を取得し（ステップＳ１２）、ログイン要求ページをコンピュータ３に送信する（ステップＳ１３）。

【００２６】コンピュータ３では、プログラム実行部３１が、Ｗｅｂサーバ２から送信されたログイン要求ページを受信し、受信したログイン要求ページをコンピュータ３のディスプレイ３６に表示する（ステップＳ１４）。

【００２７】図５は、コンピュータ３のディスプレイ３６に表示されたログイン要求ページの表示例を示す説明図である。ディスプレイ３６には、図５（ａ）に示すように、「お客様のＩＤとパスワードを入力して下さい。」とのメッセージとともに、ＩＤ、パスワードの入力枠、「ＯＫ」ボタン、「再入力」ボタンが表示される。

【００２８】ユーザは、この表示に従ってキーボード３７を操作し、ＩＤ、パスワードの入力枠に、それぞれＩＤ、パスワードを入力する。ＩＤ又はパスワードを間違えたとき、ユーザは、「再入力」ボタンをクリックし、ＩＤ又はパスワードを入力し直す。正しければ、「ＯＫ」ボタンをクリックする。

【００２９】「ＯＫ」ボタンがクリックされたとき、プログラム実行部３１は、ＩＤ及びパスワードをＷｅｂサーバ２に送信する（ステップＳ１５）。Ｗｅｂサーバ２では、情報送受信処理部２１が、コンピュータ３からユーザのＩＤ及びパスワードを受け取る（ステップＳ１６）。

【００３０】第一認証処理部２２は、予め記憶されているユーザＩＤ及びパスワードを、データベースインタフ

ェース２５を介してデータベース２６から取り出し、受け取ったユーザＩＤ及びパスワードを、予め記憶されているユーザＩＤ及びパスワードと照合する（ステップＳ１７）。

【００３１】図２に示すように、データベース２６には、ユーザＡのＩＤ、パスワードとして、それぞれ「ａｂｃ１２３」、「ＲＥＳＵＯＮＯＴＮＯＨ」が記憶されている。受け取ったＩＤが「ａｂｃ１２３」であり、パスワードが「ＲＥＳＵＯＮＯＴＮＯＨ」であるときは、照合した結果、受け取ったＩＤ及びパスワードは、データベース２６に記憶されたＩＤ及びパスワードと一致する。一致したとき、第一認証処理部２２は、第一認証が成功したと判定する（ステップＳ１８）。

【００３２】一方、受け取ったＩＤが「ａｂｃ１２３」であり、パスワードが「ＲＥＳＵＯＮＥＳＩＮ」であるときは、照合した結果、受け取ったＩＤ及びパスワードは、データベース２６に記憶されたＩＤ及びパスワードと一致しない。一致しなかったとき、第一認証処理部２２は、第一認証不成功と判定する。

【００３３】第一認証が不成功と判定されたとき、情報送受信処理部２１は、再度、確認のため、ログイン要求ページをコンピュータ３に送信し（ステップＳ１３）、送信されたユーザＩＤ及びパスワードを受け取って（ステップＳ１６）、照合を行い（ステップＳ１７）、第一認証成功か否かの判定を行う（ステップＳ１８）。

【００３４】所定回数、第一認証が不成功に終わったとき、ログインを要求した者は、不正にアクセスした者とみなしてこの処理を終了させる。このようにして、不正なアクセスが防止される。

【００３５】第一認証が成功したとき、確認コード生成部２３が、確認コードを自動生成する（ステップＳ１９）。確認コードは、数値、文字、記号のいずれか、あるいはこれらの組み合わせによってランダムに生成される。情報送受信処理部２１は、確認コード生成部２３によって生成された確認コードを、データベース２６に記憶されている電子メールアドレスの宛先へ送信する（ステップＳ２０）。

【００３６】例えば、ユーザＡの場合、前述のように電子メールアドレスは、「user_a@ichinonet.ne.jp」になっているので、確認コードは、ユーザＡによって指定されたメールサーバ５に送信される。尚、送信した確認コードは、データベースインタフェース２５によって、データベース２６の確認コード記憶エリアに記憶される。

【００３７】ユーザは、メールを受信するため、携帯端末４を操作し、携帯端末４は、メールサーバ５にアクセスして、確認コードが記録されたメールを受信する（ステップＳ２１）。Ｗｅｂサーバ２では、情報送受信処理部２１が、取引案内ページをコンピュータ３に送信する（ステップＳ２２）。

【００３８】コンピュータ３では、プログラム実行部３１が、取引案内ページを受信し（ステップＳ２３）、この取引案内ページをディスプレイ３６に表示する。ディスプレイ３６には、図５（ｂ）に示すように、案内メッセージ「お取り引きの種別を入力して下さい。」が表示され、取引内容として、種別１～３が表示される。例えば、取引が金融機関における取引の場合、種別１～２は、残高照会、振り替え等となる。

【００３９】ユーザは、この表示に従ってキーボード３７を操作し、取引の種別を入力する。種別を間違えたとき、ユーザは、「再入力」ボタンをクリックし、正しければ、「ＯＫ」ボタンをクリックする。

【００４０】「ＯＫ」ボタンがクリックされたとき、プログラム実行部３１は、入力された取引の種別をＷｅｂサーバ２に送信し、取引依頼の要求をする（ステップＳ２４）。Ｗｅｂサーバ２では、情報送受信処理部２１が、コンピュータ３から送信された取引依頼の要求を受信する（ステップＳ２５）。

【００４１】第二認証処理部２４は、取引内容が第二認証を要するものなのかどうかを判定する（ステップＳ２６）。例えば、取引が金融機関における取引であって、取引内容が残高照会等の場合のように、セキュリティを強化すべきではないときは、第二認証を行う必要はないと判定し、第二認証を実行せずに、取引ページをコンピュータ３に送信する（ステップＳ３５）。

【００４２】一方、取引内容が自分の口座から他人の口座への振り替えの場合のように、セキュリティを強化すべき場合、第二認証処理部２４は、第二認証を行う必要があると判定する。第二認証処理部２４が第二認証を要すると判定したとき、情報送受信処理部２１に確認コード要求ページを送信する（ステップＳ２７）。

【００４３】コンピュータ３では、プログラム実行部３１が確認コード要求ページを受信する（ステップＳ２８）。図５（ｃ）に示すように、コンピュータ３のディスプレイ３６には、「確認コードを入力して下さい。」とのメッセージとともに、確認コードを入力する入力枠が表示される。

【００４４】携帯端末４では、確認コードがユーザによって取得され（ステップＳ２９）、コンピュータ３では、ユーザによって確認コードが入力され（ステップＳ３０）、入力された確認コードは入力枠に表示される。この確認コードを入れ間違えたとき、ユーザは、「再入力」ボタンをクリックし、正しければ、「ＯＫ」ボタンをクリックする。

【００４５】「ＯＫ」ボタンがクリックされたとき、コンピュータ３のプログラム実行部３１は、入力された確認コードを返信コードとしてＷｅｂサーバ２に送信する（ステップＳ３１）。

【００４６】Ｗｅｂサーバ２では、コンピュータ３から送信された確認コードを受信する（ステップＳ３２）。ここで、ユーザになりすまして、ＩＤ及びパスワードを

Ｗｅｂサーバ２に送信したとしても、この者は、データベース２６に記憶されている電子メールアドレスを知ることはできない。従って、ユーザになりすました者は、確認コードを返信することはできず、確認コードが返信されなかったとき、第二認証処理部２４は、処理を終了させる。確認コードを受信したとき、第二認証処理部２４は、送信した確認コードをデータベース２６の確認コード記憶エリアから取り出す。そして、第二認証処理部２４は、受信した確認コードを、送信した確認コードと照合する（ステップＳ３３）。

【００４７】ＩＤ及びパスワードの送り主がユーザ本人であれば、Ｗｅｂサーバ２から送信された確認コードと同じ確認コードが返信されるので、送信した確認コードと受信した確認コードとが一致することになる。確認コードが一致したとき、第二認証処理部２４は、第二認証が成功したと判定する（ステップＳ３４）。

【００４８】一方、確認コードが一致しなかったときは、入力ミスも考えられるため、再度、確認コード表示ページを送信し（ステップＳ２７）、確認コードを受信して（ステップＳ３２）、再度、照合を行う（ステップＳ３３）。そして、照合の結果、所定回数、不一致が続いたときは、ユーザ本人になりすました者が適当に確認コードをＷｅｂサーバ２に送信していることも想定されるため、第二認証は、最終的に不成功と判定し、この処理を終了させる。このようにして、なりすましが排除される。第二認証が成功したと判定されたとき（ステップＳ３４）、情報送受信処理部２１は、取引ページを送信する（ステップＳ３５）。

【００４９】コンピュータ３では、プログラム実行部３１が、取引ページを受信し、この取引ページをコンピュータ３のディスプレイ３６に表示する（ステップＳ３６）。コンピュータ３のディスプレイ３６には、図５（ｄ）に示すように、第二認証の成功メッセージとして「お客様であることを確認できました。」が表示され、ユーザとの間で取引等が開始される。

【００５０】以上説明したように、本実施の形態によれば、ＩＤ及びパスワードを受け取って第一認証が成功したときは、確認コードを自動生成して、ユーザが指定した電子メールアドレス宛て（メールサーバ５）に送信し、その応答として受信した確認コードを、送信した確認コードと照合することにより、第二認証を行うようにしたので、不正な「なりすまし」を排除してユーザ本人の確定を確実に行うことができる。これにより、インターネット上でのセキュリティを強化することができる。

【００５１】尚、本発明を実施するにあたっては、種々の形態が考えられ、上記実施の形態に限られるものではない。例えば、上記実施の形態のように、通信ネットワークは、インターネット１ではなく、イントラネット（intranet：企業内ネットワーク）であってもよい。通信ネットワークがインターネット１である場合は、ＨＴＴＰプロトコルに従ってデータを送受信できるように、Ｗｅｂサーバ２を用いたのに対し、イントラネットでは、サーバに、データを所有しているデータベースサーバ、あるいは受信した情報とデータベースとを関連づけて処理をするようなアプリケーションサーバ等を用いることもできる。これらのサーバを用いた場合には、これらのサーバが、ユーザからのアクセスに対して直接、第一認証、第二認証を行うことになる。

【００５２】コンピュータ３と携帯端末４との機能については、携帯端末４にブラウザ機能を備え、メールサーバ５に届けられたメールをコンピュータ３で受信し、各ページの受信、ＩＤ、パスワード及び確認コードの送信を携帯端末４で行えるようにすることもできる。

【００５３】確認コード生成部２３は、確認コードを必ずしもランダムに生成するように構成されたものでなくてもよく、例えば、数字、記号等を連番にして確認コードを生成するものであってもよい。

【００５４】コンピュータ３から返信する確認コードは、必ずしもＷｅｂサーバ２から送信された確認コードと同じである必要はなく、Ｗｅｂサーバ２が送信した確認コードとコンピュータ３から返信された確認コードとの間に相関がとれるようにしてあれば良い。例えば、コンピュータ３のプログラム実行部３１が確認コードの文字列を逆にして返信することもできるし、プログラム実行部３１が、所定の規則に従って（例えば、連番で）コードを作成して返信することもできる。また、Ｗｅｂサーバ２が確認コードを暗号化して送信し、受信した確認コードを復号化するようにしてもよい。

【００５５】確認コードを送るタイミングについては、上記実施の形態では、第一認証が成功したとき、すぐに送るようにしたが、第二認証が必要かどうかを判断してから送るようにしてもよい。上記実施の形態の適用対象としては、必ずしも金融機関に限られるものではなく、個人的な情報交換等も含め、様々なものに適用することができる。

【００５６】さらに、上記実施の形態では、プログラムが、それぞれメモリに予め記憶されているものとして説明した。しかしながら、これらのプログラムは、ＦＤ（Floppy Disk）、ＣＤ－ＲＯＭ（Compact Disc Read-Only Memory）、ＤＶＤ（Digital Video Disc）などのコンピュータ読み取り可能な記録媒体に格納して配布するものとしてもよい。そして、インターネット上のサーバ装置が有するディスク装置等にプログラムを格納しておき、例えば、搬送波に重畳させて、コンピュータにダウンロード等するものとしてもよい。

【００５７】

【発明の効果】以上説明したように、本発明によれば、不正を防止することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係るセキュリティシステ

ムの構成を示すブロック図である。

【図２】図１のデータベースに記憶されたユーザ認証情報の一例を示す説明図である。

【図３】図１のコンピュータのハードウェア構成を示すブロック図である。

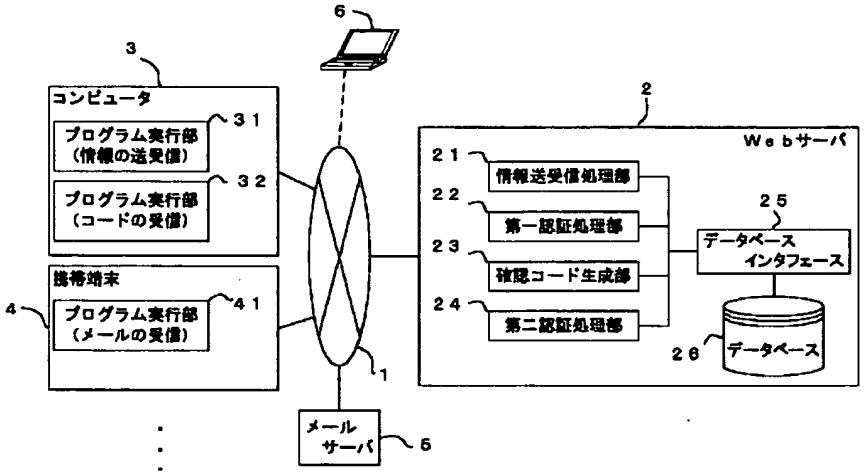
【図４】本発明の実施の形態に係るＷｅｂサーバ、コンピュータ及び携帯端末の動作を示すフローチャートである。

【図５】図１のコンピュータのディスプレイに表示された表示例を示す説明図である。

【符号の説明】

１　インターネット
２　Ｗｅｂサーバ
３　コンピュータ
４　携帯端末
５　メールサーバ
２２　第一認証処理部
２４　第二認証処理部
３１，３２，４１　プログラム実行部

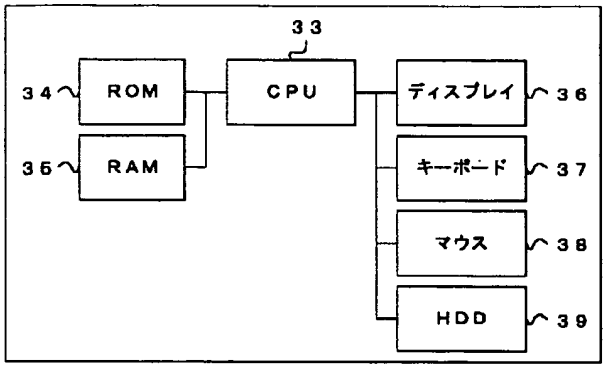
【図１】



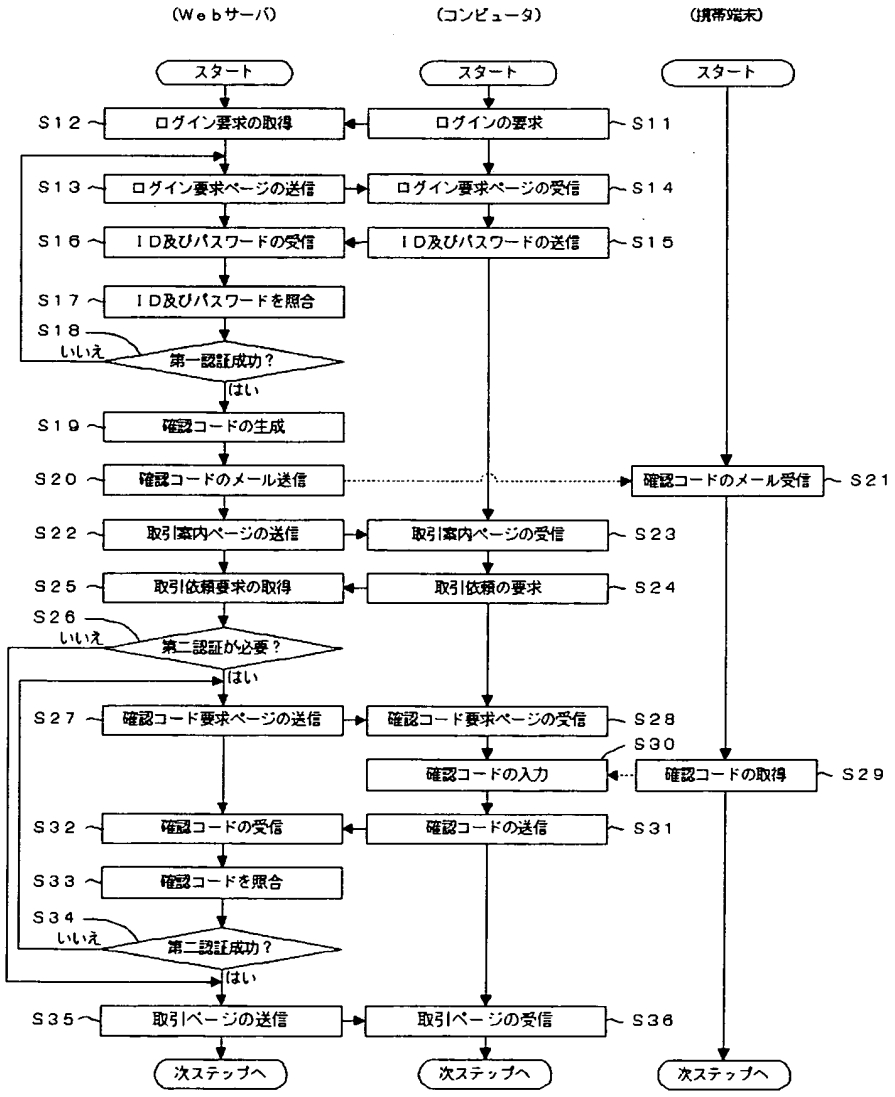
【図２】

ユーザ	ＩＤ	パスワード	電子メールアドレス	（確認コード記憶エリア）	・・・
A	abc123	********* (RESUONOTNOH)	user_a@ichinonet.ne.jp		・・・
B	efg456	*********	user_b@nino_net.ne.jp		・・・
C	hij789	*********	user_c@sannonet.ne.jp		・・・
					・・・

【図３】

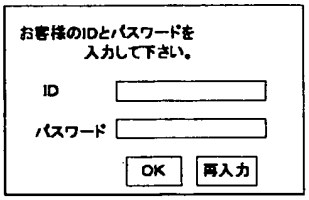

33
34
ROM
CPU
ディスプレイ
36
35
RAM
キーボード
37
マウス
38
HDD
39

【図４】

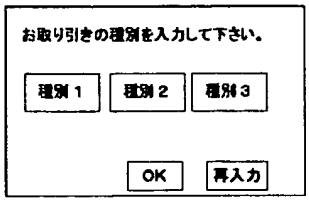

(Webサーバ)
(コンピュータ)
(携帯端末)
スタート
スタート
スタート
S12
ログイン要求の取得
ログインの要求
S11
S13
ログイン要求ページの送信
ログイン要求ページの受信
S14
S16
ID及びパスワードの受信
ID及びパスワードの送信
S15
S17
ID及びパスワードを照合
S18
いいえ
第一認証成功？
はい
S19
確認コードの生成
S20
確認コードのメール送信
確認コードのメール受信
S21
S22
取引案内ページの送信
取引案内ページの受信
S23
S25
取引依頼要求の取得
取引依頼の要求
S24
S26
いいえ
第二認証が必要？
はい
S27
確認コード要求ページの送信
確認コード要求ページの受信
S28
S30
確認コードの入力
確認コードの取得
S29
S32
確認コードの受信
確認コードの送信
S31
S33
確認コードを照合
S34
いいえ
第二認証成功？
はい
S35
取引ページの送信
取引ページの受信
S36
次ステップへ
次ステップへ
次ステップへ

【図５】

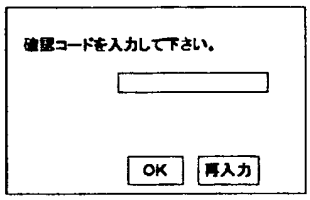
(a)


お客様のIDとパスワードを
入力して下さい。
ID
パスワード
OK
再入力

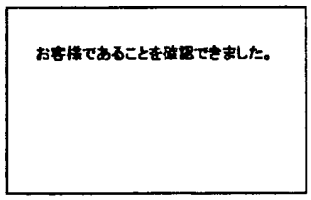
(b)


お取り引きの種別を入力して下さい。
種別１
種別２
種別３
OK
再入力

(c)


確認コードを入力して下さい。
OK
再入力

(d)


お客様であることを確認できました。